

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number:

0 365 930
A2

(12)

EUROPEAN PATENT APPLICATION

(21) Application number: 89118953.2

(51) Int. Cl.⁵ G06F 7/58

(22) Date of filing: 12.10.89

(30) Priority: 28.10.88 US 264467

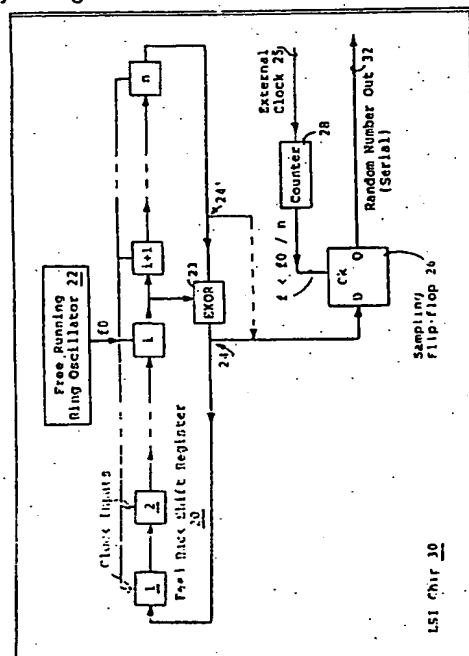
(43) Date of publication of application:
02.05.90 Bulletin 90/18(64) Designated Contracting States:
DE FR GB(71) Applicant: International Business Machines
Corporation
Old Orchard Road
Armonk, N.Y. 10504(US)(72) Inventor: Schulz, Raymond A.
8317 Morningside Drive
Manassas VA 22111(US)(74) Representative: Mönig, Anton, Dipl.-Ing.
IBM Deutschland GmbH Patentwesen und
Urheberrecht Schönaicher Strasse 220
D-7030 Böblingen(DE)

(54) Random number generator circuit.

(57) A VLSI compatible, random number generator being highly invulnerable to cryptographic attack is based upon a low frequency sampling of the output of a pseudo-random number generator which is operated at a varying frequency from a free-running ring oscillator. In a first embodiment, a free-running ring oscillator is used to drive a sampled linear feedback shift register. Because of the variations in power supply voltage and other circuit parameters over time, the frequency produced by the ring oscillator, when applied as the clocking input to the linear feedback shift register, causes the linear feedback shift register to operate in an aperiodic manner. The asynchronous, serial pseudo-random number output from the linear feedback shift register is sampled periodically, thereby introducing randomly occurring deviations from the pseudo-random number sequence. In a second embodiment of the invention, a variation of the free-running ring oscillator is employed as the pseudo-random number generator, by introducing into the feedback loop of the ring oscillator, an exclusive OR circuit which is connected so that the ring oscillator thereby produces a serial, pseudo-random number sequence. Additional uncertainty in the sequence of random numbers produced by the free-running pseudorandom number generator, is caused by the race condition which occurs at

the inputs to the exclusive OR connected in the circuit. This can cause unpredictable skipping from a first portion of the pseudo-random number sequence to a second portion of the sequence when unbalanced signal delays occur due to variations in power supply voltage.

FIG. 1.



RANDOM NUMBER GENERATOR CIRCUIT

The invention disclosed broadly relates to semiconductor circuits and, more particularly, it relates to an improved integrated circuit for random number generation.

The availability of high quality random number generators is essential to the effectiveness of a cryptographic system. With the advent of very large scale integrated circuits (VLSI), and the embodiment of cryptographic systems in VLSI, it is important that component random number generators be compatible with VLSI circuit processing. Various pseudo-random number generators have been developed in the prior art, however they are all subject to attack by an eavesdropper with the intention of circumventing the cryptographic system.

One approach in the prior art to random number generation is the use of linear feedback shift registers. For example, in the book by S. W. Glomb, "Shift Register Sequences," Holden-Day, Inc., San Francisco, 1967, describes maximum length linear feedback shift registers which satisfy several criteria for randomness. Three of those criteria are, first, that in every period, the number of ones and the number of zeros do not differ by more than one. A second criterion is that in every period half the runs have a length of one, one-fourth of the runs have a length of two, one-eighth of the runs have a length of three, and so on. Furthermore, for each of these run lengths, there are as many runs of zeros as there are runs of ones. A third criterion is that the auto-correlation function is unity for a zero shift, and minus one/n for all other shifts (n being the number of shift register stages).

As Glomb and others have pointed out, the linear feedback shift register sequence is inherently periodic, which makes the output of the shift register not truly random, but only pseudo-random. Although this diminishes its utility as a component of a cryptographic system, it has been the practice in the prior art to increase the duration of the period by using a sufficiently large number of stages in the linear feedback shift register. For example, a sixty-four bit, maximum length feedback shift register, running at a clocked frequency of one MHz, would not repeat itself for 585,000 years.

However, in cryptographic applications, the linear feedback shift register approach is vulnerable to attack because it is deterministic. All future and all past states can be predicted when the present state of the shift register is known. While it is true that the resulting output of the prior art linear feedback shift registers has superior statistical qualities, its result is unfortunately, totally predict-

able.

The invention as claimed solves the problem of providing an improved random number generator which, in particular is compatible with VLSI fabrication processes, and which can produce non-deterministic random numbers of high statistical quality.

In summary, the invention is based upon low frequency sampling of the result and the variability in the frequency of oscillation of a free-running ring oscillator. In a first embodiment, a free-running ring oscillator is used to drive a sampled linear feedback shift register. Knowledge of the shift register state is kept from the outside by sampling the linear feedback shift register at a low frequency. Infrequent sampling allows the shift register information to clear out before the next sample is taken. This minimizes the amount of information about the shift register state which gets outside. Also, because of the variations in power supply voltage and other circuit parameters over time, the frequency produced by the ring oscillator, when applied as the clocking input to the linear feedback shift register, causes the linear feedback shift register to operate in an aperiodic manner. The output of the linear feedback shift register is sampled by means of a sampling flip-flop which is driven at a periodic clock rate by an external clock signal. The asynchronous serial random number output from the linear feedback shift register is sampled in a periodic manner by the sampling flip-flop, thereby introducing randomly occurring deviations from the pseudo-random number sequence. The external clocking signal is maintained at a lower sampling frequency than the frequency of the free-running ring oscillator, and this prevents the discovery of the shift register state by an attacker. Potential race conditions at the sampling flip-flop greatly complicate any attack which might have been based on an exhaustive analysis of the output of the linear feedback shift register.

In a second embodiment of the invention, a variation of the free-running ring oscillator is employed as the pseudo-random number generator, by introducing into the feedback loop of the ring oscillator, an exclusive OR circuit which is connected so that the ring oscillator thereby produces a serial random number sequence in a manner similar to that of a conventional linear feedback shift register. This embodiment also uses low frequency sampling to minimize information about the state of the generator which gets outside. By virtue of the time varying power supply voltages and other circuit parameters, the frequency of operation of the resulting free-running pseudo-random number generator causes a non-periodic serial random

number sequence to be produced at its output. Additional uncertainty in the sequence of random numbers produced by the free-running pseudo-random number generator, is caused by the race condition which occurs at the inputs to the exclusive OR connected in the circuit. This can cause unpredictable skipping from a first portion of the pseudo-random number sequence to a second portion of the sequence when unbalanced delays occur in the free-running pseudo-random number generator due to variations in power supply voltage and other circuit parameters. A sampling flip-flop is connected to the output of the free-running pseudo-random number generator and the flip-flop is driven by a periodic external clock signal. Thus, in addition to the race condition which can occur at the sampling flip-flop due to the periodic sampling of the non-periodic pseudo-random number sequence from the free-running pseudo-random number generator, the unpredictable skipping from a first portion of the sequence to a second portion of the sequence due to the race conditions at the exclusive OR circuit, adds an additional level of unpredictability to the resultant random numbers generated by the circuit. This further complicates any attempt by an attacker to break the system and attempt to predict subsequent numbers produced by the circuit.

These and other objects, features and advantages of the invention will be more fully appreciated with reference to the accompanying figures.

Fig. 1 is an overall logic diagram of a first embodiment of the invention, a sampled linear feedback shift register random number generator, with a free-running ring oscillator.

Fig. 2 is a circuit diagram of the free-running ring oscillator 22.

Fig. 3A shows a logic diagram of a conventional D-type flip-flop such as is used in the delay elements 1, 2, etc. of the linear feedback shift register of Fig. 1.

Fig. 3B shows how the D-type flip-flop of Fig. 3A is connected, when used as a shift register element.

Fig. 4 is a circuit and logic block diagram of a second embodiment of the invention, showing the free-running pseudo-random number generator which is sampled at node B.

Fig. 5 is a variation of the circuit shown in Fig. 4, illustrating the free-running pseudo-random number generator sampled at node C.

Fig 6A shows a circuit schematic diagram of one stage A2 in the free-running pseudo-random number generator, where the stage consists of two cascaded inverters.

Fig 6B is an alternate embodiment A2' of the stage A2 for the free-running pseudo-random number generator, showing eight inverters connected in

cascade.

Fig 7 is a logic block diagram of the free-running pseudo-random number generator with four delay stages A0 through A3 and a single exclusive OR block.

Fig 8 is an alternate embodiment for the free-running pseudo-random number generator, showing eight delay stages A0 through A7 and three exclusive OR logic blocks.

Fig 9 is a logic block diagram of an exclusive OR circuit.

Fig 10 is a circuit diagram of a NAND circuit.

Fig 11A is a timing diagram illustrating the operation of the free-running pseudo-random number generator circuit of Fig. 7, for nominal delays.

Fig 11B shows the operation of the circuit of Fig. 7 with unbalanced delays.

Fig. 12 is a table illustrating the sequence of pseudo-random number values which are produced by the free-running pseudo-random number generator, and further illustrates the skipping in the sequence produced when an unbalanced delay occurs.

Fig. 13 is an example graph of the stage delay for a stage in the free-running pseudo-random number generator, as a function of the power supply voltage Vdd.

Fig. 14 is an example graph showing the voltage Vdd of the power supply 40 as it varies over time.

Fig. 1 is a logic block diagram of the first embodiment of the invention, of a sampled linear feedback shift register random number generator, with a free-running ring oscillator. The N-stage linear feedback shift register 20 consists of a serially connected sequence of shift register elements which can be, for example, D-type flip-flops such as are shown in the circuit diagram of Fig. 3A, connected with the "Q" output from a previous stage applied to the "D" input of the next stage, as is illustrated in the schematic diagram of Fig. 3B. The shift register stages 1, 2, ..., i, i+1, ..., n of the linear feedback shift register 20 of Fig. 1, are clocked by the ring oscillator 22 having an output frequency f0, as is shown in the schematic diagram of Fig. 2. The free-running ring oscillator 22 can be for example a cascaded sequence of complementary MOS inverters as shown in Fig. 2. The drain voltage Vdd and the ground potential Gnd are supplied by the power supply 40 as shown in Fig. 2. Power supplies are never made to produce a perfectly constant DC voltage, and a typical power supply voltage diagram is shown in Fig. 14. Typical power supplies used for powering large scale integrated circuits will operate at a tolerance of approximately ± 10 percent. In a CMOS technology where the nominal Vdd to ground potential difference is 5 volts, the variation in the power supply

voltage over time will be approximately ± 0.5 volts. The frequency of the voltage variation is random and is produced by noise on the power supply and supply lines itself, and is also produced by on-chip noise sources 40, which include the switching of other circuits on the same semiconductor chip. The aggregate of all such switching and noise is a relatively high frequency randomly changing noise waveform which is added to the constant nominal value for the power supply voltage Vdd. Reference to Fig. 13 will illustrate the consequence of having a time varying value for Vdd from the power supply 40. Fig. 13 is a graph of the delay per inverter stage in a cascaded inverter sequence of a ring oscillator, as a function of variations in the power supply voltage Vdd. It can be seen that even in the best case BC for CMOS inverter ring oscillator, that the delay per stage can vary by approximately 10 percent when the power supply voltage varies by approximately 10 percent. In the worse case depiction WC for circuit behavior shown in Fig. 13, the variation can be larger than ± 10 percent. As a consequence, the frequency f0 produced by the ring oscillator 22 is not a constant value but varies in an unpredictable manner.

When the frequency f0 from the ring oscillator 22 is used to clock the D-type flip-flop delay elements in the linear feedback shift register 20 of Fig. 1, the result is that the rate of production of pseudo-random numbers in the bit stream output by the linear feedback shift register varies over time. The output of the linear feedback shift register 20 can be connected at the node 24 which is the output of the exclusive OR 23, or alternately it can be connected to the input node 24 to the exclusive OR 23 which is connected to the output of the Nth or last stage of the linear feedback shift register 20.

In either case, the output of the linear feedback shift register 20 is connected to the D input of the D-type flip-flop 26 which is used to sample the output of the linear feedback shift register.

Linear feedback shift registers are well-known in the prior art to produce pseudo-random number sequences. This is described for example in an article by F. J. MacWilliams, et al., in an article entitled "Pseudo-Random Sequences and Arrays," Proceedings of the IEEE, Vol. 64, No. 12, December 1976, pp. 1715-1730. In the MacWilliams, et al. article, a number of example pseudo-random number generators based upon linear feedback shift registers are described. The linear feedback shift register produces a serial bit stream whose binary numeric value is a sequence of pseudo-random numbers which have a natural period of repetition. The larger the number of delay stages in the linear feedback shift register used in the pseudo-random number generator, the larger will be the number of

pseudo-random numbers in the sequence before the periodic repetition occurs. If an attacker is able to identify the type of linear feedback shift register being employed to produce the pseudo-random number sequence, and if the attacker is able to intercept one of the pseudo-random number values, the attacker will then be able to predict the next occurring pseudo-random number values by knowing where the generator is in the production of the pseudo-random number sequence.

However, in accordance with the invention, sampling the D flip-flop 26 at a low frequency prevents the attacker from seeing every bit of the shift register. The idea is to sample at a low frequency so that all the bits can be flushed through before another sample is taken. This minimizes the information that can get to the outside world. In addition, by introducing a race condition at the sampling flip-flop 26, a degree of unpredictability is created in the production of pseudo-random number values so that an attacker will find it more difficult to predict next values based merely on the interception of an existing produced value. This is accomplished by sampling the asynchronous output of the pseudo-random number values from the linear feedback shift register of Fig. 1, with a periodic sampling signal produced by an external clock on line 25. A periodic external sampling signal is input on line 25 and its frequency can be reduced by applying it to the counter 28, so that an effective clocking signal is output from the counter 28 and applied to the clock input of the D-type flip-flop 26. The frequency f of the clocking signal applied by the counter 28 to the sampling flip-flop 26 should be smaller than the frequency with which the linear feedback shift register will cycle a signal from its first stage 1 through its last stage N, that is f should be less than f0 divided by n. The low frequency sampling by the external clock signal prevents discovery of the shift register state, which would be needed by an attacker to break the system. The counter 28 logic circuits will fail to respond (because they are not fast enough) if an attacker attempts to run the external clock frequency high enough to sample every shift register bit. The resultant sampled values for the pseudo-random number sequence produced by the linear feedback shift register 20, are then output at the Q output of the sampling flip-flop 26, on the random number output line 32. This is a serial bit stream which represents a pseudo-random number sequence which has an unpredictable sequence of values, by virtue of the periodic sampling of the asynchronous output of the linear feedback shift register 20.

The vulnerability of the circuit of Fig. 1 to attack by an eavesdropper is minimized further by physically positioning the circuit of Fig. 1 on an

integrated circuit chip 30 so as not to allow any of the linear feedback shift register 20 to be made available at an input/output pin on the chip. This can be done by allowing no testing of the shift register stages in the linear feedback shift register 20, such as conventional level sensitive scan design (LSSD) testing. In addition, the ring oscillator frequency for the free-running ring oscillator 22, must not be related to the external input clock on line 25 which is applied to the counter 28. This is accomplished by making the ring oscillator 22 inaccessible from outside the chip. One way to make the circuit of Fig. 1 difficult to tamper with is to form it on the bottom side of the chip, as is the custom with flip chip bonding technology.

In circumstances where an all-zeros condition may occur in the delay stages 1 through N of the linear feedback shift register 20 of Fig. 1, during the powering up of the circuit, or alternately as a noise transient condition, additional peripheral circuitry can be included to detect and correct for the all-zeros condition.

Fig. 4 shows a second embodiment of the invention which is a free-running pseudo-random number generator which has the feedback loop from the cascaded delay stages of the ring oscillator 22 of Fig. 1, connected through an exclusive OR stage 44 to produce the pseudo-random number sequence. This is shown in Fig. 4 where a cascaded sequence of inverter stages A0 through A3 are connected to form the sequence of delay stages in the free-running pseudo-random number generator 42. The output node C from the circuit 42 is connected as one input to a two-input exclusive OR 44. The other input E to the exclusive OR 44 is connected to the output of one of the delay stages A1 through A3 of the circuit 42. This topology is the same as that for a conventional linear feedback shift register and the binary bit stream at either node B or node C will be a pseudo-random number sequence. Node B can then be employed as the output node in Fig. 4 which is connected over line 43 to the D input of a D-type flip-flop 26, in a manner similar to that described for the circuit of Fig. 1.

The operation of the free-running pseudo-random number generator circuit of Fig. 4 has an additional feature which is not present in the sampled linear feedback shift register embodiment of Fig. 1. Occasionally, a race condition will occur between the two inputs to the exclusive OR circuit 44, due to the unbalanced delays which can occur in the delay stages A0 through A3 for the circuit 42, due to the time variation of the power supply voltage from the power supply 40. This can be shown by an example of the operation of the free-running pseudo-random number generator of Fig. 4, as is illustrated in Figs. 11A, 11B and 12. The

free-running pseudo-random number generator circuit of Fig. 4 can be simplified in its illustration by using a logic diagram such as that in Fig. 7, which depicts the respective stages A0 through A3 as simple delay blocks in a linear feedback shift register representation. Fig. 12 is a table showing the sequence of pseudo-random number values which will occur during normal operation of the circuit of Fig. 7. As can be seen, there is a natural periodicity of 15 states of four binary bits per state, before the sequence is repeated. The normal operation for states 3, 4 and 5 is shown in Fig. 11A, where nominal delays have occurred in the delay stages A0 through A3. In the fifth state, the expression produced by the circuit of Fig. 7 is 0110. The delay stage A1 will apply a binary value one (x) to a first input E of the exclusive OR 44 and the delay stage A0 will apply a binary value zero to the second input C of the exclusive OR 44. Under normal operation, this will produce an exclusive OR output at B of a binary one and this can be seen as the first bit (x3) for the state 6 of the pseudo-random number sequence in Fig. 12. However, if an unbalanced delay occurs in the signal propagation in the stages A0 through A3, due to a time variation in the power supply value Vdd or due to other variations in circuit parameters, a race condition can occur at the two inputs E and C to the exclusive OR 44. For example, if the output on E from the stage A1 is delayed with respect to the output on C from the stage A0, as is illustrated in Fig. 11B, then the exclusive OR circuit 44 can erroneously produce a binary value of zero at its output. This is shown in the table of Fig. 12 where the state following state 5 is no longer the intended state 6 of the binary sequence 1011 for the pseudo-random number sequence, but instead becomes state 13, that is it becomes the binary sequence 0011. This unpredictable shift in the position of the pseudo-random number sequence creates an additional level of unpredictability in the pseudo-random number sequence produced by the circuit, in accordance with the invention.

The output of the free-running pseudo-random number generator 42 is applied over line 43 to the sampling flip-flop 26, at the D input. The flip-flop 26 is driven at a periodic clock frequency by the external clock signal on line 25, through the counter 28. The frequency of clocking should be less than the frequency F for the production of pseudo-random number values which have cycled through the full complement of delay stages A0 through A3. In other words, the sampling flip-flop 26 circuit samples at a frequency whose period is longer than the duration required for a signal to propagate through all the delay stages A0, A1, A2 and A3 in circuit 42. The synchronous sampling of the asynchronously produced bit stream on line 43 by the

sampling flip-flop 26, produces the same type of unpredictability in the output on the output line 32 as was described previously for the sampled linear feedback shift register embodiment of Fig. 1.

The invention of Fig. 4 thus has two sources for random production of pseudo-random number values, the first being the race condition which occurs at the inputs to the exclusive OR 44 and the second is the race condition which occurs between the asynchronous occurrence of signals on line 43 and the periodic sampling signal from the input clock line 25, as they are applied to the sampling flip-flop 26. The resulting pseudo-random number sequence has a level of unpredictability which makes it very difficult for an attacker to anticipate subsequent values produced by the circuit.

Fig. 6A shows a two inverter per stage ring oscillator delay stage element A2. The delay stages A2, etc. should, at a minimum, be at least two inverters connected in cascade. Any even number of inverters will be sufficient to produce the desired delay per stage with the preservation of the polarity of the signal between the input and the output of the delay stage. The number of inverters per stage can be increased and Fig. 6B shows an eight inverter per stage example A2". It has been found that between six to ten inverters per stage provide a reasonably good operation for the invention. Each delay element A0, A1, A2, A3 of Fig. 4 must have a sufficiently fast rise and fall time characteristic so that the steady state for an input signal is always reached before the next input signal transition begins. Otherwise, the effective delay of each element A0, A1, A2, A3 will be reduced. If this were to happen, the arrival times of the signals at the inputs to the exclusive OR 44 will be disturbed. Proper response can be assured by requiring that the time duration of each delay stage A0, A1, A2 and A3 is sufficiently long, which can be achieved by having a sufficiently long delay-to-rise time ratio in each delay element. The delay-to-rise time ratio for each element A0, A1, A2 and A3 should be at least three-to-one, and more like five-to-one. Thus, each delay stage A0, A1, A2 and A3 in the circuit 42 of Fig. 4 should optimally consist of at least six, but perhaps more like ten inverters per stage, depending upon the semiconductor technology employed to form the circuits on the integrated circuit chip 30.

Fig. 5 is a variation of the circuit of Fig. 4, which is sampled at the node C, instead of the node B, as is shown in Fig. 4. Such sampling is logically the same, since the value of a binary signal which starts at node B and propagates through the cascaded sequence of stages A3, A2, A1 and A0 in the circuit 42, will ultimately be produced with the same polarity at the node C.

Fig. 8 is another embodiment for the circuit 42

of Figs. 4 and 5, which employs eight delay stages A0 through A7, instead of the four delay stages shown in Figs. 4 and 5. It can also be seen that three exclusive OR circuits 44, 44' and 44" are provided in the circuit of Fig. 8 instead of the single exclusive OR circuit as is shown in Fig. 7. The variety of linear feedback shift register configurations which can be embodied in the free-running pseudo-random number generator circuit 42, is a wide variety, as is indicated by the examples shown in the MacWilliams, et al. article referenced above. In each example pseudo-random number generator, the time variation of the power supply voltage as applied to the inverters making up the delay stages in the circuit 42, will produce race conditions which will occur at the inputs of each exclusive OR device 44, 44', 44", etc., producing the unpredictable skipping from a first portion of the pseudo-random number sequence to a second portion, in accordance with the invention.

Fig. 9 is a logic block diagram of an exclusive OR circuit which is comprised of four NAND two-input devices connected as shown. This is an example of an exclusive OR circuit 44.

Fig. 10 is a circuit schematic diagram of a CMOS circuit for producing a NAND logic function such as would be used in the NAND logic blocks of Fig. 9.

The resulting invention produces unpredictable sequences of pseudo-random numbers which prevent an attacker from anticipating subsequent values in the output bit stream. This finds particular application in cryptography where the production of random numbers which are not predictable, is essential in the creation of master key values used for cryptographic operations. The invention disclosed herein produces a reliable source of unpredictable random number sequences which can be employed for high security applications in cryptography.

Although specific embodiments of the invention have been disclosed, it will be understood by those having skill in the art that changes can be made to those specific embodiments without departing from the spirit and the scope of the invention.

Claims

1. A random number generator circuit, formed on an integrated circuit chip, said chip having power supply voltage which randomly varies with respect to time, comprising:
a plurality of n delay stages serially connected in a sequence with an input at a first stage in said sequence and an output at a last stage in said sequence, each stage including at least two inverter circuits, each inverter circuit having a power

supply input terminal;
 an exclusive OR circuit coupled in a feedback path between said output of said last stage and said input of said first stage;
 said plurality of n delay stages being divided into a first subplurality of i stages, having an output coupled as a first input to said exclusive OR circuit;
 said plurality of n delay stages having a second subplurality of n minus i stages in said plurality of stages, with an output coupled as a second input to said exclusive OR circuit;
 said exclusive OR circuit generating a pseudorandom signal pattern in response to inputs from said first and second subpluralities of delay stages;
 each said delay stage in said plurality of n delay stages propagating signals which traverse consecutive ones of said delay stages, each said delay stage applying a randomly varying magnitude of signal propagation delay to said signals in response to said randomly varying power supply voltage applied to said delay stages, resulting in randomly occurring race conditions between said first and second inputs of said exclusive OR circuit;
 said exclusive OR circuit randomly changing said pseudo-random signal pattern in response to said randomly occurring race conditions;
 an output terminal coupled to said feedback path, for outputting said randomly changing pseudo-random signal pattern.

2. The random number generator circuit of claim 1, which further comprises:

a sampling circuit having an input connected to the output of said second subplurality of stages, for periodically sampling the binary state at the output of said second subplurality of stages;
 whereby said sampling circuit outputs a pseudo-random signal pattern which randomly changes with time.

3. The apparatus of claims 1 or 2, wherein said sampling circuit samples at a frequency whose period is longer than the duration required for a signal to propagate through said n delay stages.

4. The random number generator circuit of claim 1, which further comprises:

a sampling circuit having an input connected to the output of said exclusive OR circuit, for periodically sampling the binary state at the output of said exclusive OR circuit;
 whereby said sampling circuit outputs a pseudo-random signal pattern which randomly changes with time.

5. The apparatus of claims 1 or 4, wherein said sampling circuit samples at a frequency whose period is longer than the duration required for a signal to propagate through said n delay stages.

6. A random number generator circuit, formed on an integrated circuit chip, said chip having a power supply voltage which randomly varies with

respect to time, comprising:

a free-running ring oscillator, having a plurality of inverter circuits connected in cascade and having an output, each inverter circuit having a power supply input terminal;

a feedback shift register having a plurality of n delay stages serially connected in a sequence with a feedback path, each stage having a clock input connected to said output of said ring oscillator, said stages being divided into a first subplurality of i stages, having an output coupled as a first input to an exclusive OR device;

said feedback shift register having a second subplurality of n minus i stages in said plurality of stages, with an output coupled as a second input to said exclusive OR circuit;

a sampling circuit having an input coupled to said feedback path, for periodically sampling the binary state of a pseudo-random signal pattern output by said exclusive OR circuit;

each said inverter circuit in said ring oscillator propagating an oscillator signal which traverses consecutive ones of said inverter circuits, each said inverter circuit applying a randomly varying magnitude of signal propagation delay to said oscillator signal in response to said randomly varying power supply voltage applied to said inverter circuits, resulting in an oscillator signal output from said ring oscillator with a randomly varying frequency;
 said sampling of said pseudo-random signal pattern by said sampling circuit randomly changing in response to said randomly varying ring oscillator frequency;

whereby said sampling circuit outputs a pseudo-random signal pattern which randomly changes with time.

7. The apparatus of claim 6, which further comprises:

said sampling circuit having an input connected to the output of said second subplurality of stages, for periodically sampling the binary state at the output of said second subplurality of stages;
 whereby said sampling circuit outputs a pseudorandom signal pattern which randomly changes with time.

8. The apparatus of claims 6 or 7, wherein said sampling circuit samples at a frequency whose period is longer than the duration required for a signal to propagate through said n delay stages.

9. The apparatus of claim 6, which further comprises:

said sampling circuit having an input connected to the output of said exclusive OR circuit, for periodically sampling the binary state at the output of said exclusive OR circuit;

whereby said sampling circuit outputs a pseudo-random signal pattern which randomly changes with time.

10. The apparatus of claims 6 or 9, wherein said sampling circuit samples at a frequency whose period is longer than the duration required for a signal to propagate through said n delay stages.

5

10

15

20

25

30

35

40

45

50

55

8

FIG. 1.

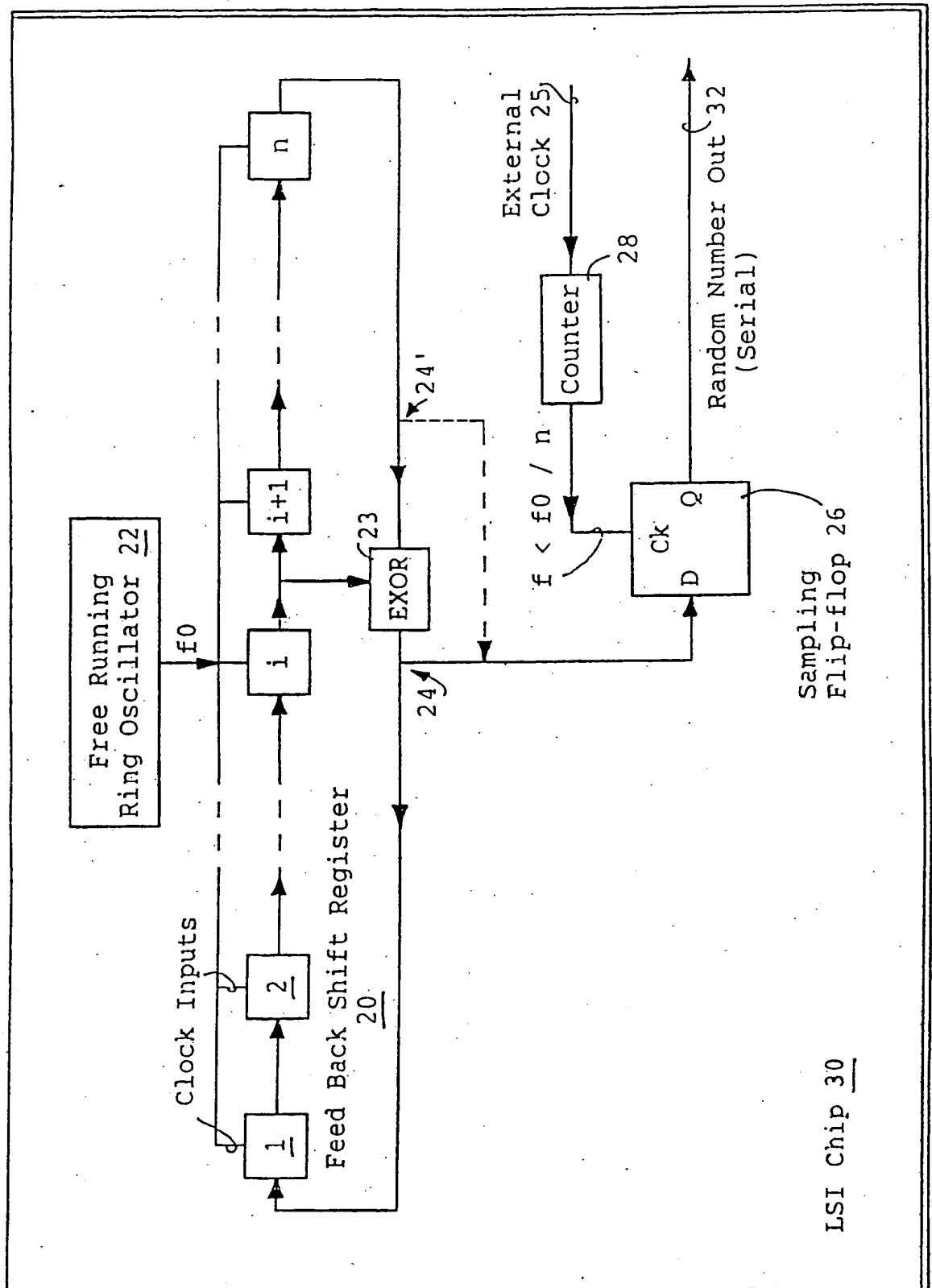


FIG. 2.

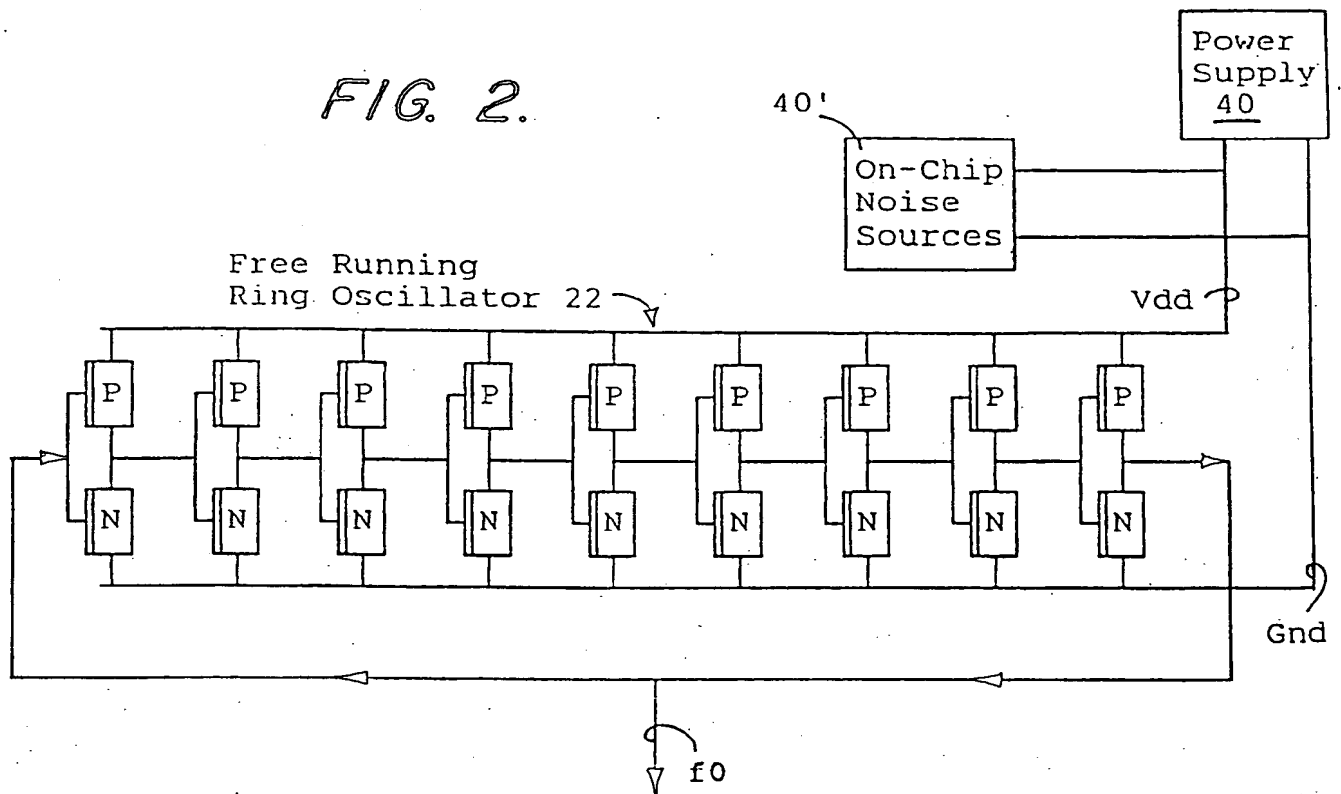


FIG. 3A.

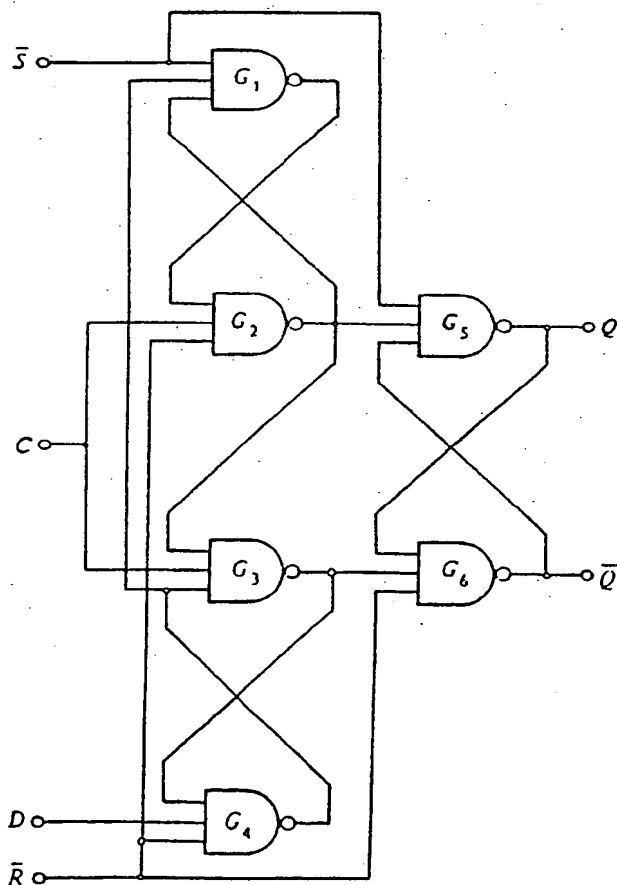


FIG. 3B.

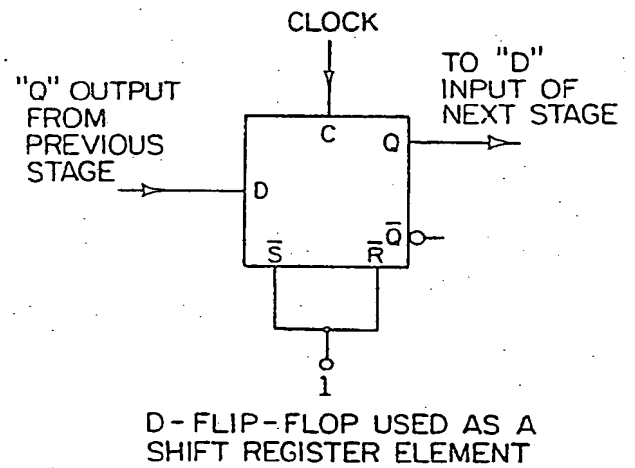


FIG. 4.

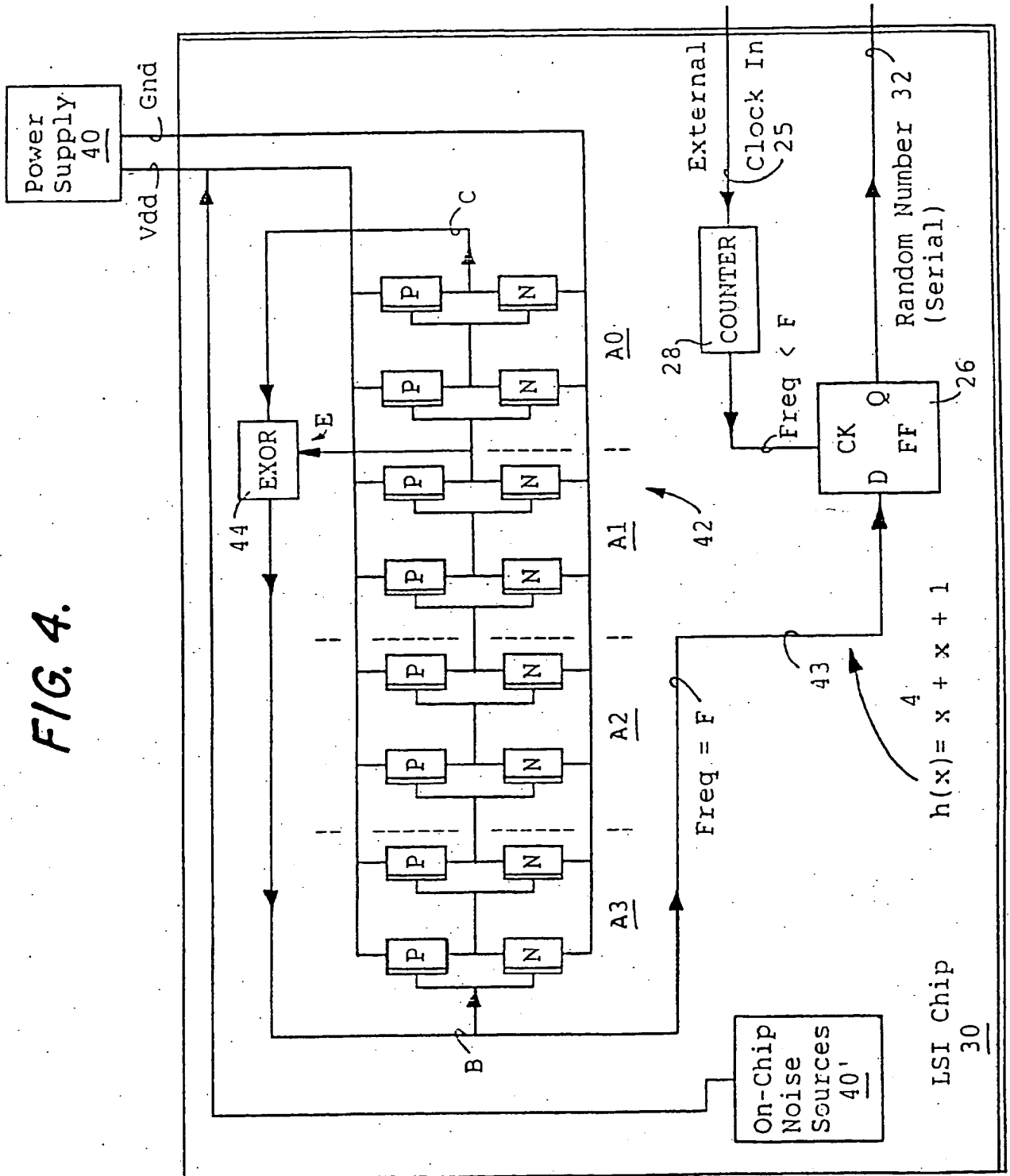


FIG. 5.

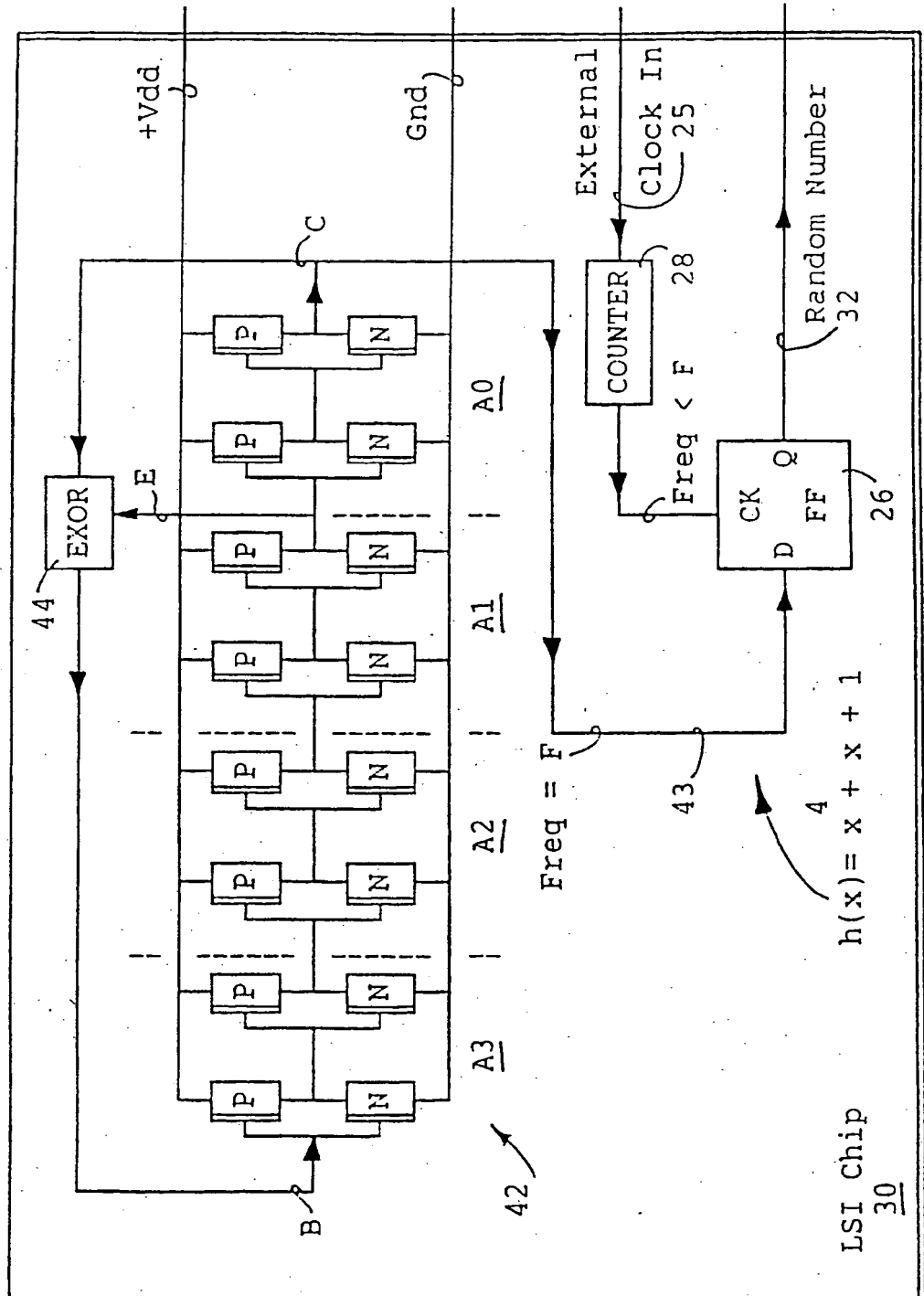


FIG. 6A.

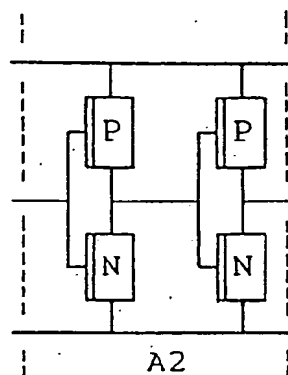


FIG. 6B.

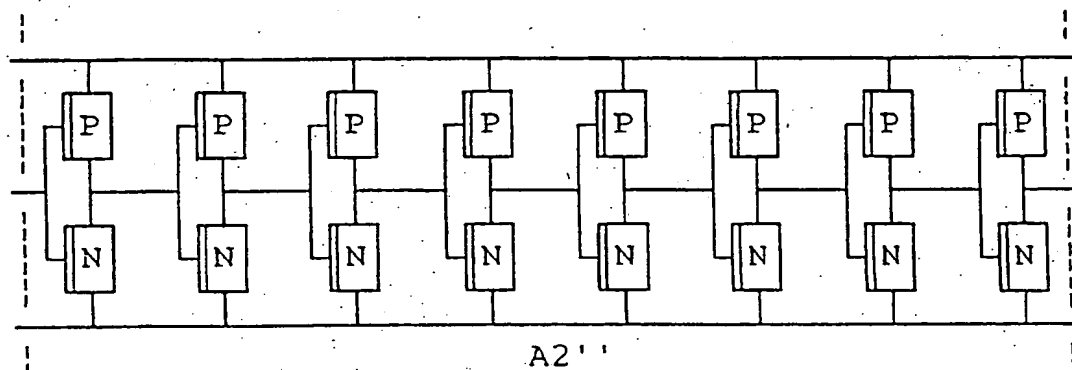


FIG. 7.

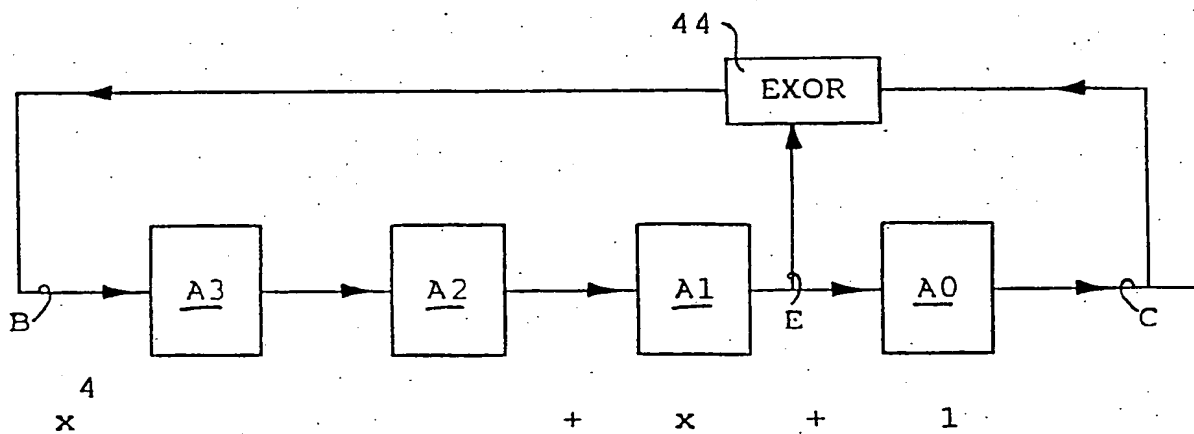


FIG. 8.

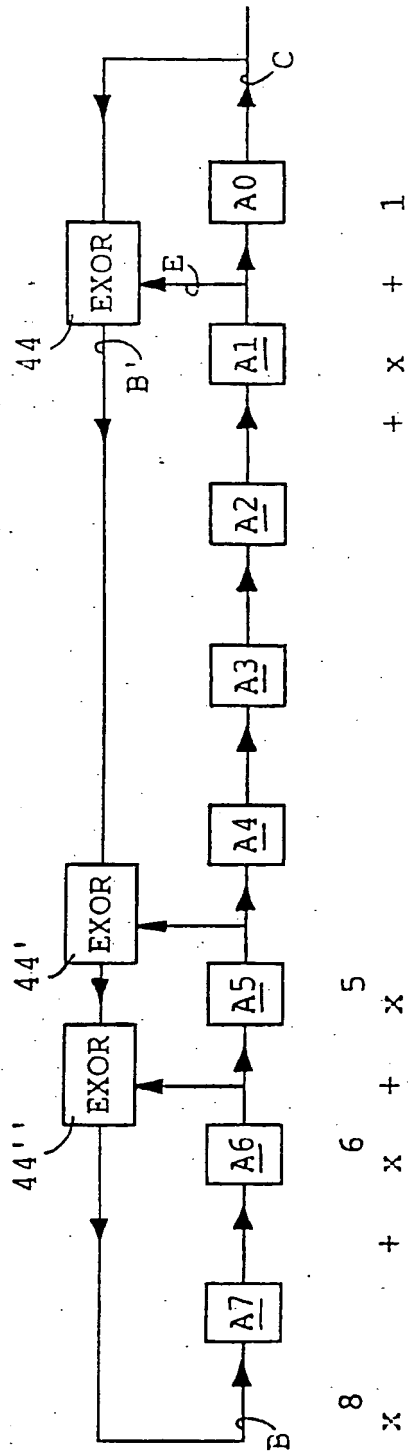


FIG. 9.

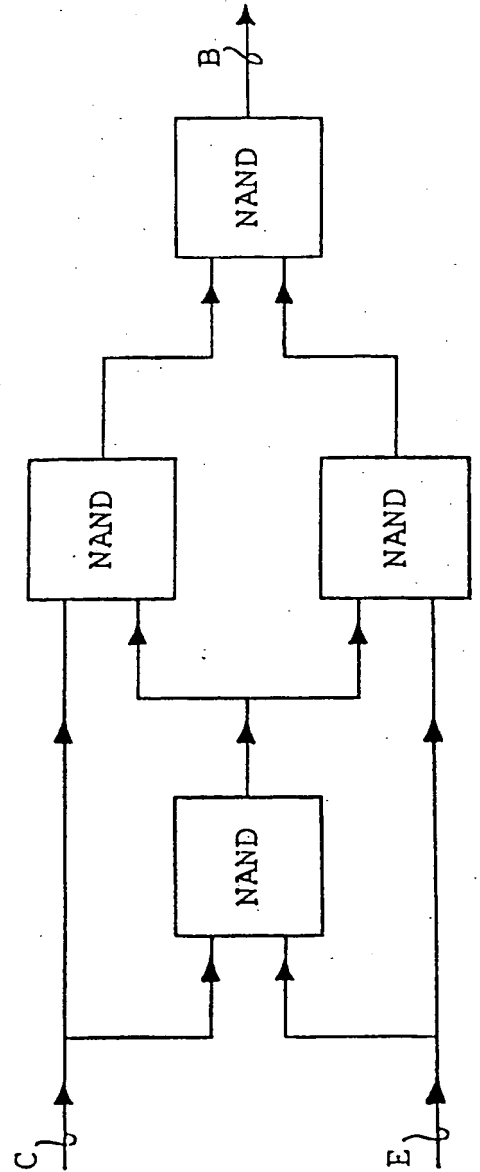
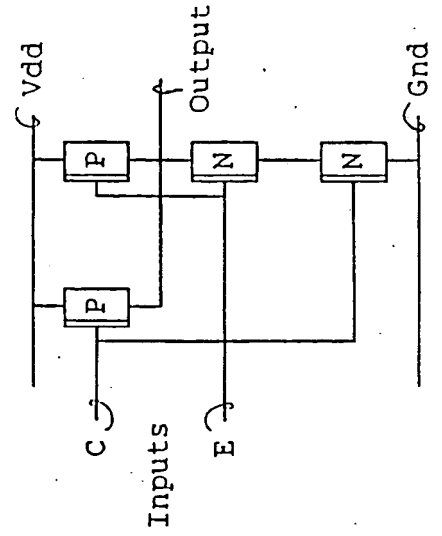


FIG. 10.



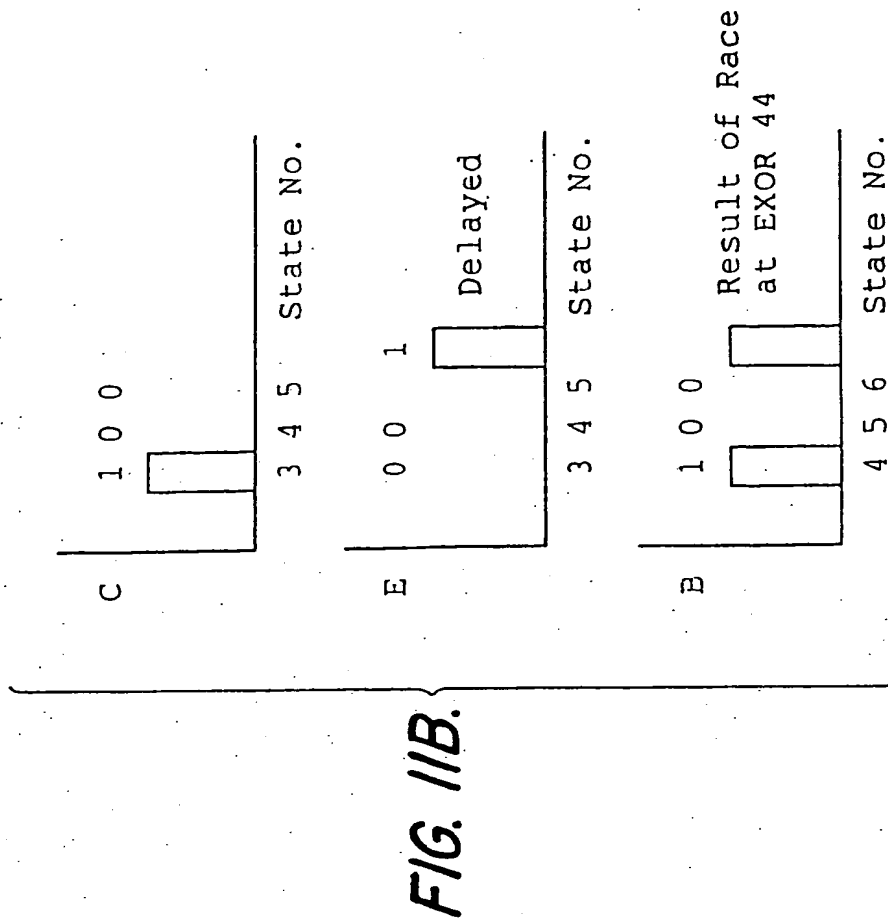
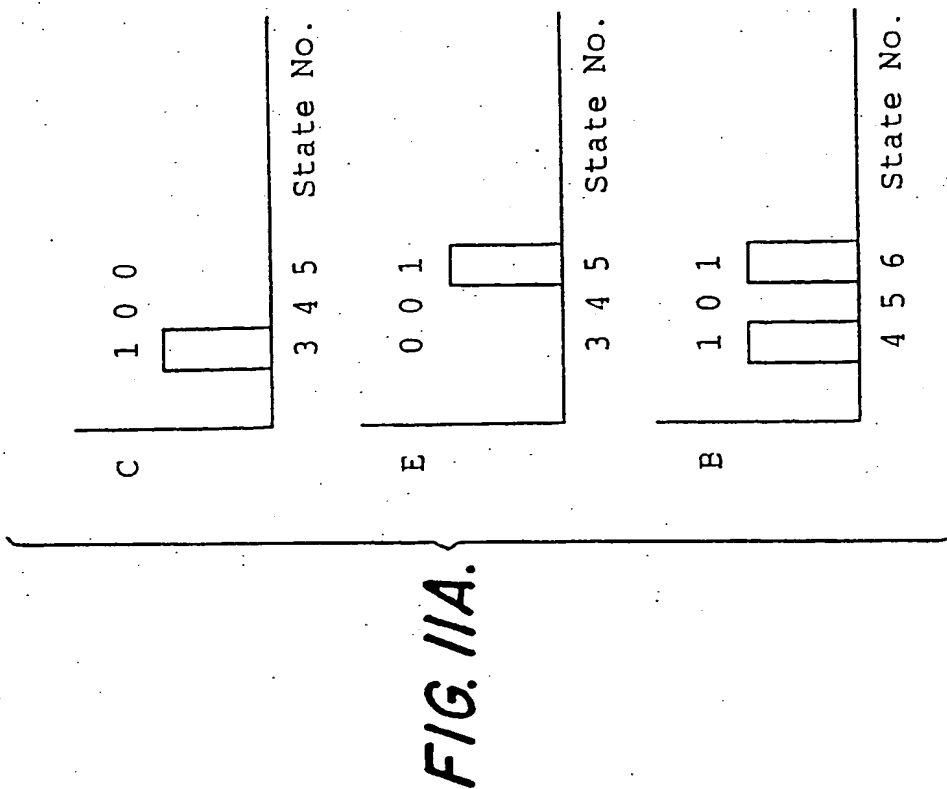
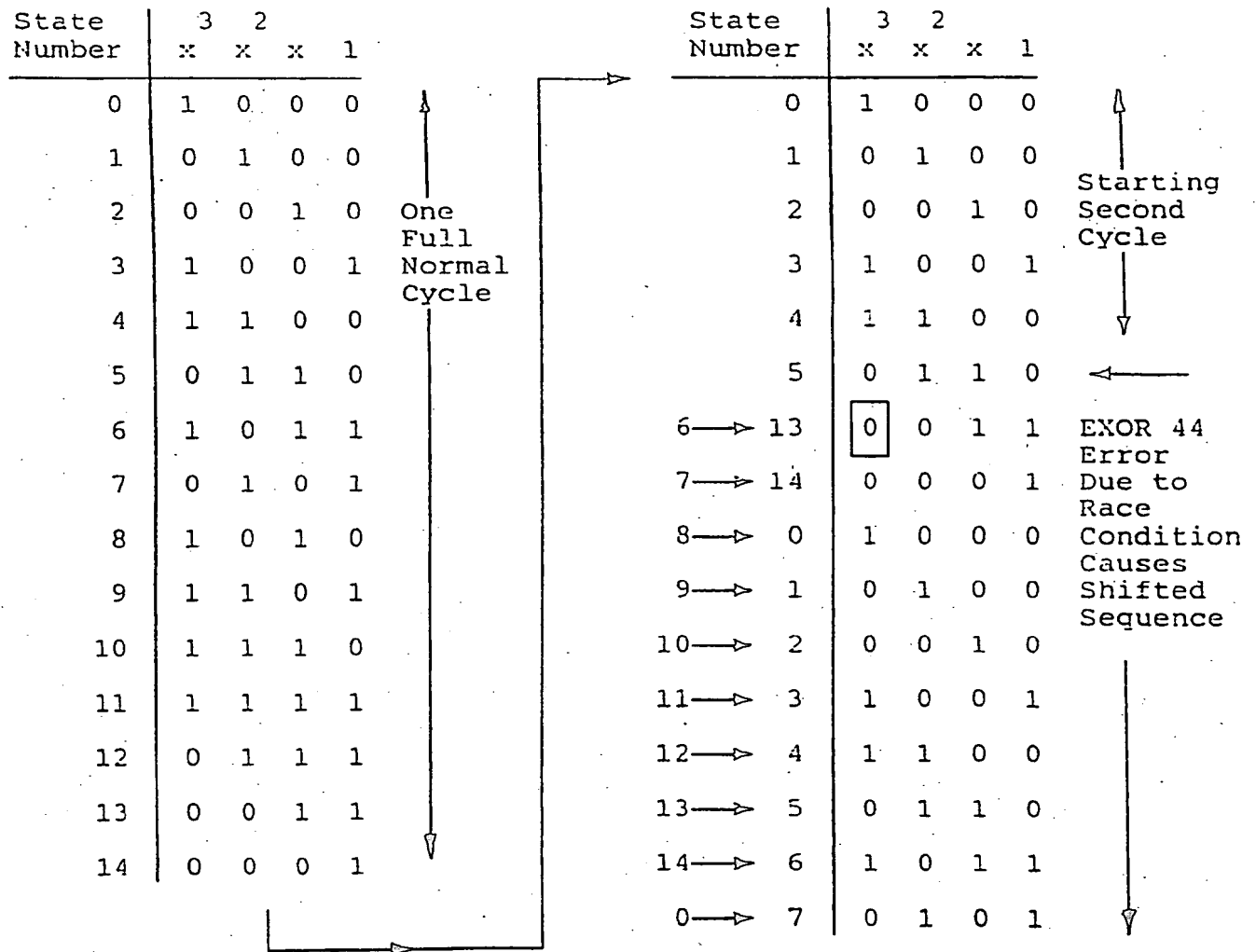


FIG. 12.



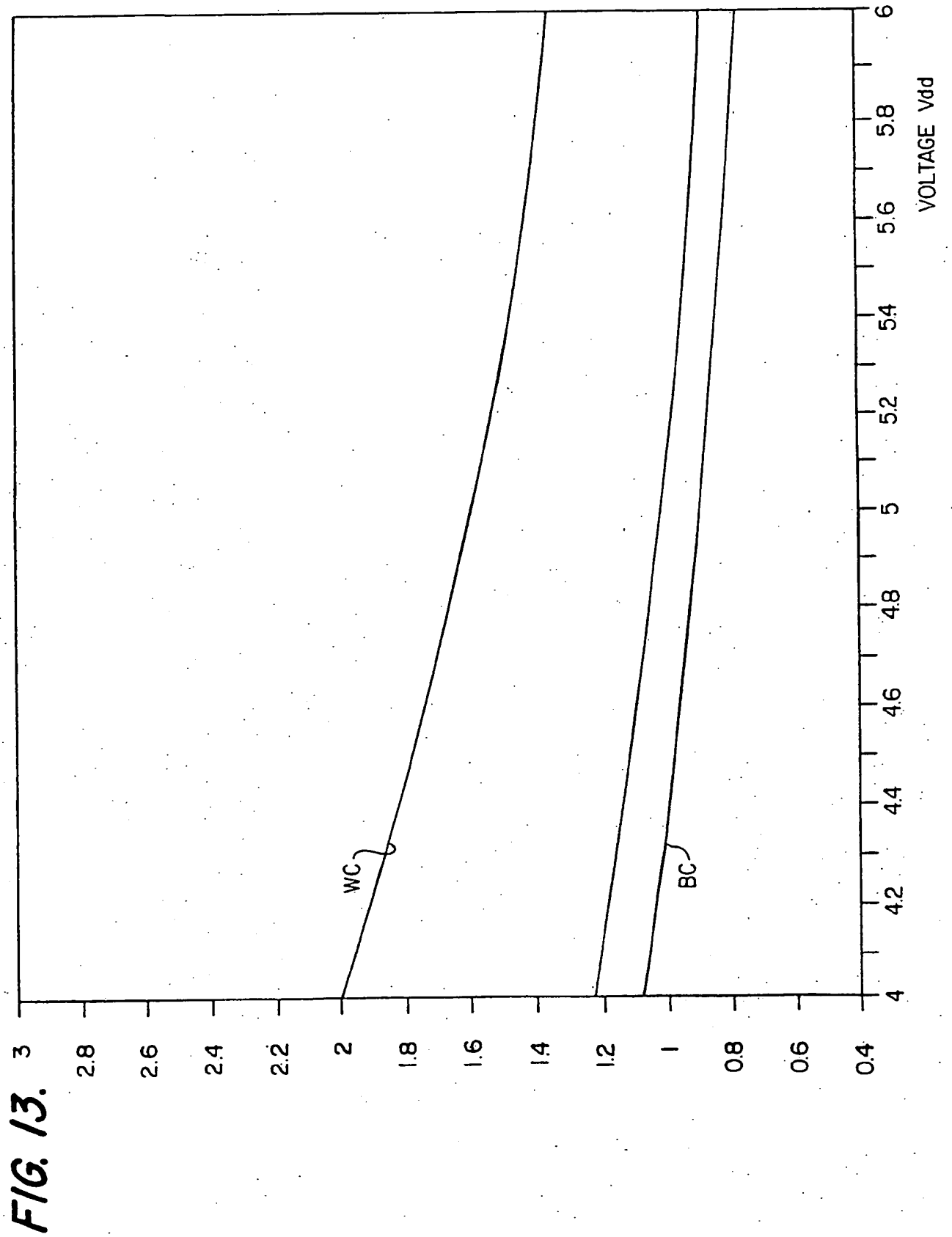
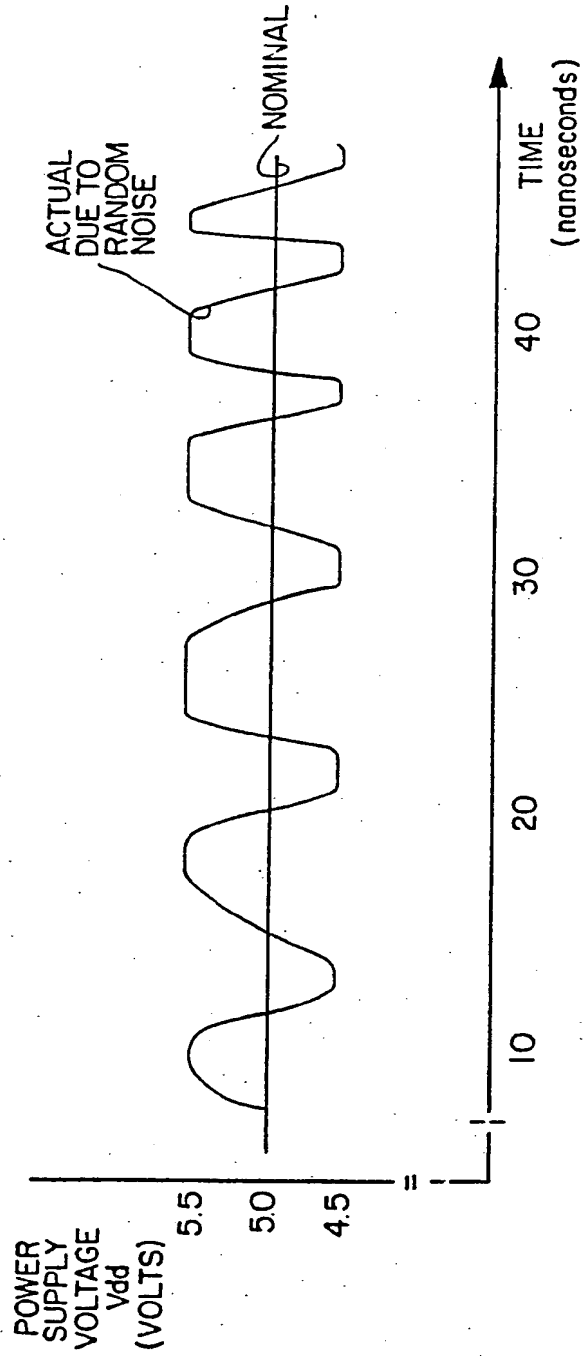


FIG. 14.



(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) Publication number:

0 365 930 A3

(12)

EUROPEAN PATENT APPLICATION

(21) Application number: 89118953.2

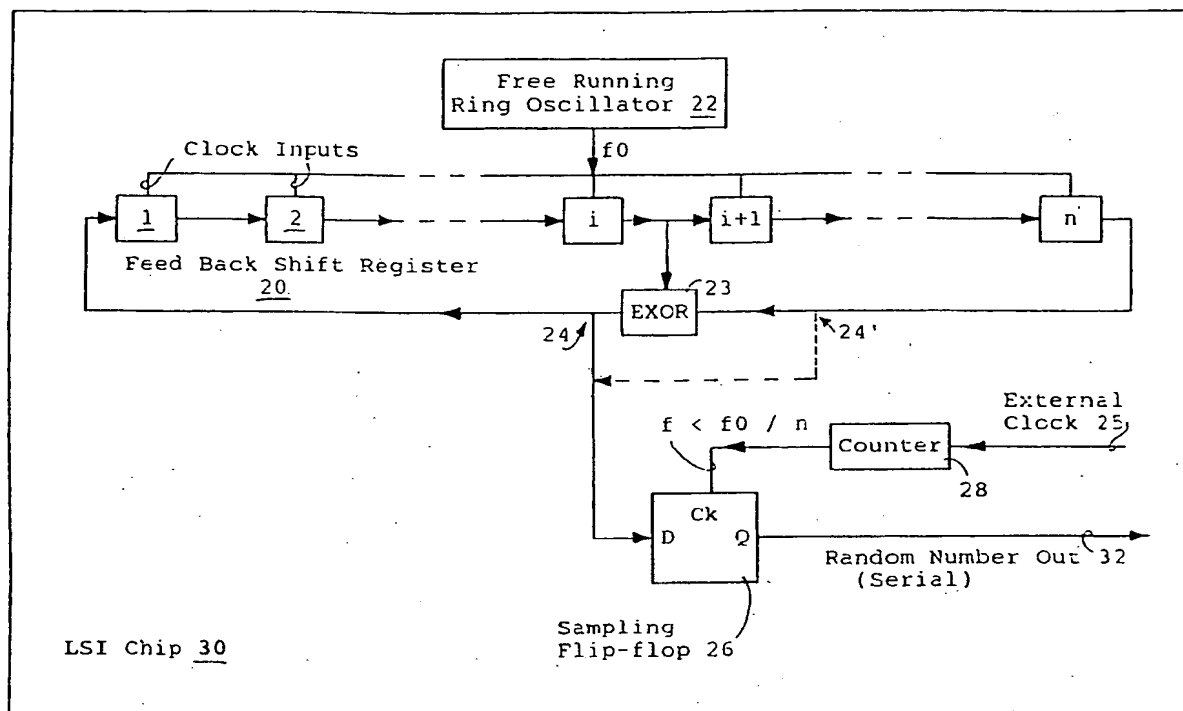
(51) Int. Cl.5: **G06F 7/58**(22) Date of filing: **12.10.89**(30) Priority: **28.10.88 US 264467**(43) Date of publication of application:
02.05.90 Bulletin 90/18(84) Designated Contracting States:
DE FR GB(88) Date of deferred publication of the search report:
29.04.92 Bulletin 92/18(71) Applicant: **International Business Machines Corporation**
Old Orchard Road
Armonk, N.Y. 10504(US)(72) Inventor: **Schulz, Raymond A.**
8317 Morningside Drive
Manassas VA 22111(US)(74) Representative: **Mönig, Anton, Dipl.-Ing.**
IBM Deutschland GmbH Patentwesen und
Urheberrecht Schönaicher Strasse 220
W-7030 Böblingen(DE)(54) **Random number generator circuit.**

(57) A VLSI compatible, random number generator being highly invulnerable to cryptographic attack is based upon a low frequency sampling of the output of a pseudo-random number generator which is operated at a varying frequency from a free-running ring oscillator. In a first embodiment, a free-running ring oscillator is used to drive a sampled linear feedback shift register. Because of the variations in power supply voltage and other circuit parameters over time, the frequency produced by the ring oscillator, when applied as the clocking input to the linear feedback shift register, causes the linear feedback shift register to operate in an aperiodic manner. The asynchronous, serial pseudo-random number output from the linear feedback shift register is sampled periodically, thereby introducing randomly occurring deviations from the pseudo-random number

sequence. In a second embodiment of the invention, a variation of the free-running ring oscillator is employed as the pseudo-random number generator, by introducing into the feedback loop of the ring oscillator, an exclusive OR circuit which is connected so that the ring oscillator thereby produces a serial, pseudo-random number sequence. Additional uncertainty in the sequence of random numbers produced by the free-running pseudorandom number generator, is caused by the race condition which occurs at the inputs to the exclusive OR connected in the circuit. This can cause unpredictable skipping from a first portion of the pseudo-random number sequence to a second portion of the sequence when unbalanced signal delays occur due to variations in power supply voltage.

EP 0 365 930 A3

FIG. 1.





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number

EP 89 11 8953

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	US-A-4 769 777 (BITTLE et al.) * Abstract; column 3, line 20 - column 4, line 31; figures 3,4 *	1-5	G 06 F 7/58
A	DE-A-2 649 502 (GÜNTHER WULFF-APPARATEBAU) * Claim 1 *	1-5	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G 06 F
The present search report has been drawn up for all claims.			
Place of search THE HAGUE		Date of completion of the search 18-09-1991	Examiner COHEN B.
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 150 (03.82) (P0401)



CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

- ☐ All claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for all claims.
- ☐ Only part of the claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claims:
- ☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions, namely:

See Sheet B.

- ☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.
- ☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:
- ☒ None of the further search fees has been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims,

namely claims: 1-5



European Patent
Office

EP 89 11 8953 -B-

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims 1-5: Variable power-supply on LFSR to generate race-conditions in feedback loop of random number generator
2. Claims 6-10: Variable power-supply on ring-oscillator to vary sampling behaviour of random number generator sampler

This Page Blank (uspto)